A METHOD OF AUTHENTICATING DIGITALLY ENCODED PRODUCTS WITHOUT PRIVATE KEY SHARING

Abstract

A method and a corresponding system for authenticating software products are proposed. A digital certificate (260) and a corresponding private key (265) required to sign each product are stored on a server computer. Whenever a user needs to sign a product, he/she logs on a client computer and transmits a corresponding request to the server computer. The server computer verifies whether the request has been received from an authorized subject; for example, an address of the client computer and an identifier of the user are compared with a predefined list (245). If the result of the verification is positive, the product is signed and returned to the client computer. For this purpose, a script (250) called on the server computer includes either an instruction passing the access password to a signing tool (255) as a parameter or an instruction causing the signing tool (255) to import the access password from a registry of the server computer.